DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services
7500 Security Boulevard, Mail Stop N2-14-26
Baltimore, Maryland 21244-1850

CENTERS FOR MEDICARE & MEDICAID SERVICES (CMS)
Office of Information Services (OIS)
Systems Security Group (SSG)
7500 Security Blvd
Baltimore, MD 21244-1850

CMS Information Security Certification and Accreditation (C&A) Procedure

Version 1.0

May 12, 2005

Table of Contents

1.0 INTRODUCTION 1

1.1 PURPOSE 1
1.2 SCOPE 1
1.3 DESCRIPTION 1
1.4 ROLES AND RESPONSIBILITIES 1
1.4.1 SYSTEM OWNER 2
1.4.2 SYSTEM MAINTAINER / DEVELOPER 2
1.4.3 CHIEF INFORMATION OFFICER (CIO) 2
1.4.4 DESIGNATED APPROVING AUTHORITY (DAA) 2
1.4.5 DIRECTOR SYSTEM SECURITY GROUP ((SSG) Senior Agency Information Security Official) 2
1.4.6 Senior Agency Information Security Official 3
1.4.7 COMPONENT ISSO / SSO 3
1.4.8 CMS C&A EVALUATOR 3

2.0 C&A PROCEDURE MATRIX 4

2.1 PRE-CERTIFICATION PHASE 4
2.2 INITIATION PHASE 6
2.3 SECURITY CERTIFICATION TASKS 15
2.4 SECURITY ACCREDITATION PHASE 22
2.5 CONTINUOUS MONITORING PHASE 26
2.6 RE-AUTHORIZATION PHASE 31

APPENDIX A –C&A FLOWCHARTS 34

APPENDIX B – CERTIFICATION INTENSITY LEVEL 41

APPENDIX C - ACRONYMS 70

APPENDIX D - C&A METHODOLOGY GROUPS AND C&A PROCEDURAL ROLES 69

1.0 INTRODUCTION

The Certification and Accreditation (C&A) Procedure documents the C&A process in place at CMS. This procedure has been developed to:

- Ensure consistency in the evaluation of security controls.
- Facilitate security accreditation decisions.
- Identify and define principle C&A roles and responsibilities.

1.1 PURPOSE

The purpose of the C&A Procedure is to establish a standard process for C&A independent of the Life-Cycle status of the system. The system test and risk assessment of a system verify the correctness and effectiveness of security controls and their ability to ensure adequate security. This process is an integral part of risk management, which continues throughout the System Life-Cycle.

This procedure defines the security assessment approach based on standard guidelines.

1.2 SCOPE

This procedure applies to all persons responsible for conducting elements of the C&A process for systems of all classifications and sensitivity levels. This document serves as a primary resource to guide and ensure consistency in completing the C&A process.

1.3 DESCRIPTION

The C&A Procedure provides sufficient detail for each phase and ensures consistent definition for the roles and responsibilities required to complete the process successfully.

The C&A process consists of six (6) interrelated phases:

- Pre-certification Phase.
- Initiation Phase.
- Security Certification Phase.
- Security Accreditation Phase.
- Continuous Monitoring Phase.
- Re-authorization Phase.

Each phase requires one or more activities. These activities define the steps to be conducted according to the C&A methodology. The steps defined in this CMS C&A Procedure matrix are illustrated in the CMS C&A Flow Chart in Appendix A. Appendix B defines the certification levels based on the system sensitivity level. Appendix C defines the acronyms used in this document.

1.4 ROLES AND RESPONSIBILITIES

This section lists the responsibilities assigned to the roles involved throughout the C&A process. Attachment D also defines the roles and responsibilities in association with the C&A

Methodology, at a high level and serves as a correlation between the two documents terms and definitions of the roles. The following roles list the responsibilities for the tasks carried out within this procedure document:

1.4.1 SYSTEM OWNER

- Completes the Business Risk Assessment (RA) of system during the SDLC process.
- Ensures the Information Security RA (IS RA) is in place and up-to-date.
- Develops and maintains the System Security Plan (SSP).
- Ensures and certifies system security meets CMS standards.
- Ensures system security is monitored and documented on an on-going basis and reports the security status to authorizing officials.

1.4.2 SYSTEM MAINTAINER / DEVELOPER

- Serves as the point of contact for the C&A process for the system.
- Develops and maintains the IS RA.
- Monitors and reports on-going efficacy of the system security.
- Collaborates with the Component Information System Security Officer (Component ISSO) to design and implement security controls and mechanisms necessary for the system to meet CMS standards and requirements.
- Collaborates with System Owner to review ST&E Rules of Engagement and ST&E Work Plan.
- Collaborates with System Owner to ensure the availability of resources necessary to conduct components of C&A process.

1.4.3 CHIEF INFORMATION OFFICER (CIO)

- Ensures CMS has a C&A process in place and that it is implemented for all systems.
- Approves or denies system Accreditation.
- Requires system re-authorization for a particular system based on Director SSG recommendations.

1.4.4 DESIGNATED APPROVING AUTHORITY (DAA)

- Approves or denies system Accreditation with authority granted by the CIO.

1.4.5 DIRECTOR SYSTEMS SECURITY GROUP ((SSG) SENIOR AGENCY INFORMATION SECURITY OFFICIAL)

- Implements the C&A program as required by the CIO.
- Determines when and at which certification level the system must undergo C&A.
- Develops and implements the C&A Project Plan.
- Designates the CMS C&A Evaluator.

- Approves the estimated level of effort to complete the C&A process.
- Coordinates the activities between the System Owner and the CMS C&A Evaluator.
- Reviews certification and continuous monitoring outputs.
- Makes accreditation recommendations to the CIO.
- Manages secure storage of C&A documentation.

1.4.6 SENIOR AGENCY INFORMATION SECURITY OFFICIAL

- Assists System Owner with technical certification of the system IS RA and SSP
- Assists System Owner in the review of the system Corrective Action Plan (CAP)

1.4.7 COMPONENT ISSO / SSO

- Assists System Maintainer / Developer in developing a CAP in response to system configuration changes.
- Assists System Maintainer / Developer in addressing deficiencies in security controls and mechanisms.

1.4.8 CMS C&A EVALUATOR

- Coordinates C&A ST&E planning with SSG and System Owner, including but not limited to time line and resource requirements.
- Conducts the ST&E specific tasks, including but not limited to updating the ST&E report.
- Assists SSG by developing accreditation recommendations for the CIO.

2.0 C&A Procedure Matrix

2.1 Pre-Certification Phase

This phase comprises the four tasks required to begin certification activities. CMS processes and resource documents are available for meeting the requirements of the Pre-Certification tasks. The following table identifies the tasks, roles, responsibilities and resources (product and reference) that support the Pre-Certification Phase.

TASK	ROLES	RESPONSIBILITIES	PRODUCT & REFERENCE
		BUSINESS RISK ASSESSMENT	
1.	System Owner	➢ System Maintainer / Developer: ♦ Ensures the completion of a Business RA of the system and development of the Business RA Report during the Business Case Analysis or Acquisition phase of the SDLC. • Products of the Business RA are; > A determination of the current risk remaining after the implementation of security controls for the business function; > Recommendations for additional or different safeguards; and > A determination of the residual risk expected to remain after the implementation of recommended safeguards.	Product: • CMS Business RA Report. Reference: • *CMS Business Risk Assessment Methodology* (RAM). • SDLC.
		DEVELOP SYSTEM SECURITY PLAN	
2.	System Maintainer / Developer	➢ System Maintainer / Developer: ♦ Ensures the development of a SSP for the system during the Requirements Analysis Phase of the SDLC: • Completes the SSP by the end of the SDLC Development Phase. • SSP documents the security requirements for the system, and the internal controls implemented or planned for implementation.	Product: • SSP Reference: • SDLC

TASK	ROLES	RESPONSIBILITIES	PRODUCT & REFERENCE
		♦ Includes the Business RA Report as an attachment to the SSP.	• SSP • CMS RA Report
PERFORM INFORMATION SECURITY RISK ASSESSMENT			
3.	System Maintainer / Developer	➢ System Maintainer / Developer: ♦ Ensures the performance of an IS RA. ♦ Ensures the production of the IS RA Report during the Development Phase of the SDLC. • The end products of the IS RA are: > An identification of vulnerabilities within the system; > A determination of the current risk remaining after the implementation of internal controls; > Recommendations for additional or different safeguards; and > A determination of the residual risk expected to remain after implementation of the recommended safeguards. • Appends the IS RA to the SSP as an attachment.	<u>Product:</u> • CMS IS RA Report • Updated SSP Reference: • SDLC • *Information Security Risk Assessment Methodology* (IS RAM)
4.	System Maintainer / Developer System Owner	➢ System Maintainer / Developer • Delivers a copy of the SSP, with the attachments, to the System Owner. ➢ System Owner • Delivers the SSP with attachments to SSG for secure file.	

2.2 Initiation Phase

The Initiation Phase consists of a number of tasks. Collectively, these tasks ensure that:

1. Adequate and timely information is provided for the CMS C&A Evaluator to complete the required tasks;
2. All parties with roles and responsibilities for the C&A process receive notification of the pending certification evaluation;
3. All parties with roles and responsibilities for the C&A process are provided with an opportunity to prepare for the certification evaluation, and allocate or obtain the resources required to complete the certification evaluation; and
4. The System Owner accepts the SSP and expected level of residual risk before the CMS C&A Evaluator begins the ST&E process.

Specific system information is necessary in order to complete the Initiation Phase. A substantial portion of this information is derived from the SSP and its attachments, the Business RA Report and the IS RA Report. If any of these documents, or their information content, is incomplete or out-of-date, the System Owner and the System Maintainer / Developer must ensure the updating and / or completion of the relevant documents before proceeding with the C&A process.

TASK	ROLES	RESPONSIBILITIES	PRODUCT & REFERENCE
CERTIFICATION PREPARATION			
1.	SSG	Prepare the C&A Project Plan Draft. ➢ SSG: ➢ Develops the draft C&A Project Plan: • Includes the identification of the following items: > Specific tasks; > Key personnel; > Milestones; > Deliverables; > Delivery schedules; > Level of effort; and > Resource requirements.	Product: • C&A Project Plan Draft

TASK	ROLES	RESPONSIBILITIES	PRODUCT & REFERENCE
2.	System Maintainer / Developer	Verify that the system is fully identified and documented in the SSP. ➢ System Maintainer / Developer: ♦ Verifies that the SSP includes: • The official system name and acronym for the system; > A unique System of Records, Financial Management Investment Board, or Web Support Team number; > The organization responsible for the system; > Contact information for the System Owner, Business Owner, SSP Author, and System Maintainer Manager; > An assignment of security responsibility; > The system operational status with respect to the SDLC; > A general description and brief statement of purpose for the system; > A diagram showing the architecture of the system and the network topology; > A description of system interdependencies, interconnections, and information sharing; > A listing of the applicable laws, regulations, directives, policies, or standards affecting security of the system and information; > A description of the types of information processed, stored, or transmitted by the system; and > A description of the physical environment in which the system operates.	Reference: • SDLC • SSP Methodology

TASK	ROLES	RESPONSIBILITIES	PRODUCT & REFERENCE
3.	System Maintainer / Developer	Verify that the security category of the system is correctly documented within the SSP. ➢ System Maintainer / Developer: ♦ Verifies that the SSP includes the following: • Designations for the data sensitivity level; • The system criticality level; and • The overall system security level.	Reference: • CMS Information Security Levels Document.
4.	System Maintainer / Developer	Verify that threat identification information is documented within the Business RA Report and the IS RA Report. ➢ System Maintainer / Developer: ♦ Reviews both RA reports to verify that potential threats are correctly identified and documented ♦ Attaches both reports to the SSP.	Reference: • *CMS Threat Identification Resource* • CMS Business RAM.
5.	System Maintainer / Developer	➢ System Maintainer / Developer: ♦ Verifies that the security controls implemented or planned for implementation for the system are correctly identified and documented within the SSP. • Ensures the SSP includes a description of the management, operational, and technical security controls implemented, or planned for implementation. ♦ Reviews the Management Controls, Operational Controls, and Technical Controls sections of the SSP to verify that internal controls are correctly identified and documented.	Reference: • *CMS Information Security Acceptable Risk Safeguards* (ARS) • *CMS Information Security Policy Handbook* • *CMS Business Partners Systems Security Manual*
6.	System Maintainer / Developer	Verify that flaws or weaknesses in the system that could be exploited by potential threats are identified and documented within the SSP. ➢ System Maintainer / Developer: ♦ Verifies that vulnerability identification information is documented within the IS RA Report and attached to the	Reference: • Questionnaires. • On-site Interviews. • Document Reviews. • Previous RA documents.

TASK	ROLES	RESPONSIBILITIES	PRODUCT & REFERENCE
		SSP. ♦ Verifies that proper procedures have been followed to identify potential vulnerabilities within the system, including but not limited to the use of: • Questionnaires; • On-site interviews; • Document reviews; • Automated scanning tools; and • Manual penetration testing techniques. ♦ Verify that vulnerabilities documented within the SSP are consistent with the following sources of vulnerability information: • Previous RA documentation; • Audit reports; • System anomaly reports; • Security reviews; • Self assessments; • Results of vulnerability scans and penetration tests; • ST&E reports; • Vulnerability lists; and • Security group and vendor advisories, alerts, and bulletins.	• Audit Reports. • System Anomaly Reports. • Security Reviews. • Self-Assessments. • Vulnerability scan and pen test reports. • ST&E Reports. • Vulnerability Lists. • Advisories, Alerts and Bulletins.
7.	System Maintainer / Developer	Verify the determination and documentation of expected residual risk to CMS operations and assets within the SSP. ➢ System Maintainer / Developer: ♦ Confirms that the Business RA and IS RA Reports document the expected residual risk, and are included within the SSP.	Reference: • CMS RA.
8.	System Maintainer / Developer	➢ System Maintainer / Developer: ♦ Delivers current SSP and attachments to System Owner. ➢ System Owner:	

TASK	ROLES	RESPONSIBILITIES	PRODUCT & REFERENCE
		♦ Reviews, approves or collaborates with System Maintainer / Developer to modify the SSP and attachments. ♦ Delivers updated SSP and attachments to SSG for secure file.	
		NOTIFICATION	
9.	SSG	➢ SSG: ♦ Identifies the CMS C&A Evaluator. ♦ Notifies the CIO, CMS C&A Evaluator, Senior Agency Information Security Official, and Component ISSO that the system is undergoing security C&A. • Notification may be sent via electronic mail or via an inter-office memorandum. • Should contain language sufficient to inform the recipient that C&A will be performed for a specific system. • The notification message should describe why C&A is necessary. • Provide a general timeframe for when the certification evaluation is to take place and when an accreditation decision is expected. • Direct system owner to deliver the current SSP and attachments to SSG.	Product: • Identified CMS C&A Evaluator. • Notification of need for C&A.
		RESOURCE IDENTIFICATION	
9.	System Owner System Maintainer	➢ System Owner and System Maintainer / Developer: ♦ Estimates the level of effort required to complete the C&A process, by considering the following factors: • Size and complexity of the system; • Security levels and requirements of the system, and magnitude of harm that might result from system	Product: • Level of Effort Estimate. Reference: • SSP.

TASK	ROLES	RESPONSIBILITIES	PRODUCT & REFERENCE
	/ Developer SSG	compromise; • The security controls implemented, or planned for implementation, to protect the system; and • Specific techniques and procedures used to verify the effectiveness of the security controls. ➢ System Owner and SSG: ♦ Must agree on the level of effort necessary to complete the C&A.	• *CMS Certification and Accreditation Methodology*
10.	CMS C&A Evaluator System Owner	➢ CMS C&A Evaluator: ♦ Documents the level of effort that will be required to complete the certification evaluation. ➢ System Owner: ➢ Reviews the CMS C&A Evaluator's proposal to ensure that the level of effort is reasonably within their estimate.	<u>Product</u>: • Level of Effort Proposal.
11.	System Owner SSG CMS C&A Evaluator	➢ System Owner and SSG: ♦ If the CMS C&A Evaluator's proposal is not reasonably within the System Owner and SSG's stated estimate; • Revises the estimate and obtains approval from the CIO; or • Works with the CMS C&A Evaluator to reduce the proposed level of effort to an acceptable level. ➢ CMS C&A Evaluator: ♦ Updates the level of effort estimate after the System Owner and SSG review.	<u>Product</u>: • Updated Level of Effort Proposal / Estimate.
12.	CIO	➢ CIO: ♦ Approves or rejects the Level of Effort Proposal.	<u>Product:</u> Approved or rejected Level of Effort Proposal included within the Project Plan.

TASK	ROLES	RESPONSIBILITIES	PRODUCT & REFERENCE
13.	SSG System Owner CMS C&A Evaluator	Determines the resources required for the C&A of the system. This includes identifying supporting organizations and personnel, funding requirements, and individuals with critical skills. ➢ SSG: ♦ Identifies appropriate resources needed for the C&A effort. ➢ System Owner: ♦ Identifies appropriate resources needed for the C&A effort. ➢ CMS C&A Evaluator: ♦ Identifies appropriate resources needed for the C&A effort.	Product: Resource Identification.
14.	CMS C&A Evaluator System Owner SSG CIO	➢ CMS C&A Evaluator: ♦ Provides the SSG with updates to the C&A Project Plan for conducting the certification evaluation. ➢ System Owner and SSG: ♦ Approves the updated project plan. ♦ Submit the updated project plan to CIO for approval, before proceeding with the certification process. ➢ CIO: ➢ Authorizes the C&A project plan.	Product: • Approved C&A Project Plan.
SECURITY PLAN ANALYSIS, UPDATE AND ACCEPTANCE			
15.	CMS C&A Evaluator SSG System Owner	Analyze the SSP to determine if the expected residual risk to CMS operations and assets is accurate. ➢ CMS C&A Evaluator and SSG: ♦ Reviews the SSP and attachments to determine if the plan is complete and consistent. ♦ Based upon the limited resources available at this phase of the C&A process, determines if the expected residual risk to CMS operations and assets appear to be correct and reasonable. ♦ Recommends changes to the security controls, expected residual risk, or other section of the SSP, as necessary.	Product: Recommended Changes to the SSP. Reference: • SSP Analysis • CMS SSP Methodology • ARS • *CMS Information Security Policy Handbook* • CMS RAM • CMS IS RAM

TASK	ROLES	RESPONSIBILITIES	PRODUCT & REFERENCE
		♦ Delivers recommendations for changes to the SSP and attachments to the System Owner. ➢ System Owner: ♦ Delivers the recommendations to System Maintainer / Developer and Component ISSO.	
16.	Component System Security Officer (ISSO) System Maintainer / Developer System Owner	Update the SSP based upon the results of the independent analysis and recommendations issued by the CMS C&A Evaluator and SSG. ➢ Component ISSO: ♦ Confirms the recommendations or provides counter-recommendations to the System Maintainer / Developer. ➢ System Maintainer / Developer: ♦ Reviews the recommended changes and makes all reasonable and appropriate modifications. ♦ Performs a Cost Benefits Analysis of the modifications. ♦ Implements the reasonable modifications according to their cost. ♦ Consults with the Component ISSO prior to making any final modifications to the SSP. ♦ Schedules a meeting between all parties if the Component ISSO or System Maintainer / Developer disagrees with any of the recommendations issued by the CMS C&A Evaluator or SSG, to resolve the disagreement. ♦ Delivers the SSP and attachments to the System Owner, after completion of the SSP modifications. ➢ System Owner: ♦ Delivers the SSP and attachments to SSG.	Product: • Updated SSP Reference: • Independent SSP Analysis.
17.	SSG System Maintainer / Developer	Review the SSP to determine if the expected residual risk to CMS operations and assets is acceptable. ➢ SSG: ♦ Reviews the SSP to determine if the expected residual risk is acceptable.	

TASK	ROLES	RESPONSIBILITIES	PRODUCT & REFERENCE
	System Owner	♦ Delivers the SSP and attachments to the System Maintainer / Developer and System Owner, if the expected residual risk is not acceptable for appropriate action. ♦ Agrees to proceed to the Security Certification Phase, if the expected residual risk is acceptable. ➢ System Maintainer / Developer and System Owner: ♦ Revises the SSP to comply with the SSG's expectations for acceptable residual risk.	

2.3 Security Certification Tasks

The Security Certification Phase comprises tasks in three areas. These tasks assess the security controls of the system and determine if they are sufficient to protect the confidentiality, integrity, and availability of CMS information and systems at the level required (sensitivity levels). In addition these tasks report the risk resulting from vulnerabilities identified during the ST&E review, and provide detailed suggestions for developing CAPs to address each vulnerability.

TASK	ROLES	RESPONSIBILITIES	PRODUCT & REFERENCE
		SECURITY CONTROL VERIFICATION	
1.	CMS C&A Evaluator System Owner System Maintainer / Developer	Request and assemble all documentation, materials, and resources required for completion of the ST&E review. ➢ CMS C&A Evaluator: ♦ Develops a set of pre-requisites necessary to complete the C&A review. • The pre-requisites document includes all technical and administrative needs, including but not limited to: > Required documentation. > Network connections. > User accounts. > Computer equipment. > Workspace; and > Information storage facilities. ♦ Delivers the pre-requisites document to the System Owner. ➢ System Owner: ♦ Assembles the appropriate resources, from the System Maintainer / Developer, requested by the CMS C&A Evaluator. ➢ System Maintainer / Developer: ♦ Provide requested pre-requisites to the System Owner, for the CMS C&A Evaluation.	<u>Product</u>: • Pre-requisites Document.

TASK	ROLES	RESPONSIBILITIES	PRODUCT & REFERENCE
2.	System Owner CMS C&A Evaluator	Assemble and review previous evaluation results of the security controls implemented for the system, and determine whether previous results are suitable for reuse. ➢ System Owner: ♦ Assembles all findings, results, evidence, and documentation from previous penetration tests, RAs, self-assessments, and audits of the security controls implemented for the system. ♦ Provides information to the CMS C&A Evaluator. ➢ CMS C&A Evaluator: ♦ Reviews information to determine if any previous assessment results are suitable for reuse in the current certification evaluation.	<u>Product:</u> • Assembled previous assessment reports. Reference: • Pre-requisites document.
3.	CMS C&A Evaluator System Owner System Maintainer / Developer	Develop and authorize the ST&E Rules of Engagement. ➢ CMS C&A Evaluator: ♦ Develops the ST&E Rules of Engagement that will govern the testing and evaluation activities. • Includes all of the standard Rules of Engagement within the system-specific rules, unless the standard rules are unreasonable or inappropriate under the circumstances. • Develops system or site-specific Rules of Engagement, and includes these as an addendum to the standard RE. • The RE shall address, at a minimum; > Technical testing limitations. > Boundaries. > Administrative requirements. > Procedures. ♦ Delivers the RE to the System Owner and System Maintainer / Developer. ➢ System Owner: ♦ Delivers the ST&E Rules of Engagement to the System	<u>Product</u>: • ST&E RE • *CMS Certification and Accreditation Methodology*

TASK	ROLES	RESPONSIBILITIES	PRODUCT & REFERENCE
		Maintainer / Developer for agreement decision. ➢ System Owner, System Maintainer / Developer and CMS C&A Evaluator: ♦ Must assent to the terms of the ST&E Rules of Engagement before proceeding with the certification tasks.	
4.	CMS C&A Evaluator System Owner System Maintainer / Developer	Develop and authorize the ST&E Work Plan. ➢ CMS C&A Evaluator: ♦ Develops the ST&E Work Plan: • Includes all testing and evaluation procedures and techniques necessary to evaluate the management, operational, and technical security controls implemented to protect the system. • The ST&E Work Plan template is included within the C&A Methodology. ♦ Delivers the ST&E Work Plan to the System Owner and System Maintainer / Developer. ➢ System Owner, System Maintainer / Developer and CMS C&A Evaluator: ♦ Must agree to the test and evaluation procedures and techniques before proceeding with the certification tasks.	Product: • ST&E Work Plan. • CMS C&A Procedures. Reference: • *CMS Certification and Accreditation Methodology* • NIST 800-53A • SSP • ARS
5.	CMS C&A Evaluator	Perform system security test and evaluation. ➢ CMS C&A Evaluator: ♦ Evaluates the management, operational, and technical security controls implemented to protect the system using the testing and evaluation techniques and procedures contained in the ST&E Test Plan. ♦ Emails a daily log of the data collected via an encrypted e-mail to the remote office location of the evaluator. ♦ Determines the effectiveness of the internal controls in a particular operational environment.	Product: • Annotated Work Plan. • Analysis Tool out-puts. • Test Results. • ST&E Support Documentation. Reference: • ST&E Test Plan.

TASK	ROLES	RESPONSIBILITIES	PRODUCT & REFERENCE
		♦ Identifies vulnerabilities and weaknesses remaining in the system after the implementation of security controls. ♦ Determines the cause of the vulnerability or weakness. ♦ Considers any modifications, updates, or improvements that would mitigate and eliminate the impact of the exposure. ♦ Analyzes the CMS business risk created by the vulnerability or weakness. ♦ Maintains a running list of vulnerabilities and weaknesses identified during the ST&E process. ♦ Assigns appropriate personnel to document each.	
6.	CMS C&A Evaluator	Prepare the ST&E Report using VACAP Tracking System. ➢ CMS C&A Evaluator: ♦ Develops the ST&E Report after the onsite and offsite testing is completed to include the following: > Assessment of the risk level; > Ease of fix; > Estimated work effort for each finding; > Detailed description of each vulnerability identified during the evaluation and the resulting business risk; > Recommended corrective actions that may be taken to reduce or eliminate the vulnerabilities; > Introduction; > Executive summary; and > Completed ST&E Work Plan: ❖ Must include actual results and be attached to the ST&E Report.	Product: • ST&E Report Draft Reference: • Annotated Test Plan • Analysis Tool out-puts • Test Results • ST&E Support Documentation • *CMS Certification and Accreditation Methodology* • *CMS Reporting Standard for Security Testing* • *VACAP Tracking System User Manual and Administration Guide*
SECURITY CERTIFICATION DOCUMENTATION			
7.	CMS C&A Evaluator	Provide the System Maintainer / Developer with the ST&E Report. ➢ CMS C&A Evaluator:	Product: • Final ST&E Report.

TASK	ROLES	RESPONSIBILITIES	PRODUCT & REFERENCE
	System Maintainer / Developer	♦ Submits the ST&E Report to the System Owner and System Maintainer / Developer in draft form. ♦ Prepares and submits the final ST&E Report after a prescribed number of days (as determined in the C&A project plan) to SSG, System Owner and System Maintainer / Developer. (This includes delivery to SSG of the findings entries in VACAP Tracking System format). • Report is in accordance to CMS Reporting Standard for Security Testing. ➢ System Maintainer / Developer: ♦ Responds to the ST&E Report within a prescribed number of days (as determined in the C&A project plan), and either agrees with or refutes the vulnerability findings, or requests the CMS C&A Evaluator to make changes to the technical content. ♦ Completes certain recommendations issued by the CMS C&A Evaluator within the report before the Certification Package is finalized if there are specific opportunities to reduce or eliminate vulnerabilities in the system prior to the final security accreditation decision. ♦ May close high-risk vulnerabilities before submitting the updated SSP. • If corrective action is taken before the CMS C&A Evaluator issues the final report, the System Maintainer / Developer shall notify the CMS C&A Evaluator, who shall then update the Status section of each finding to provide evidence that certain remediation actions have been completed.	• CMS Reporting Standard for Security Testing. • VACAP Tracking System entries for findings

8.	System Maintainer / Developer Component ISSO	Develop the system CAP and update the SSP and attachments based upon the results of the ST&E, and any modifications to the security controls in the system. ➢ System Maintainer / Developer and Component ISSO: ♦ Collaborates to develop the system CAP. • The CAP shall incorporate the corrective actions recommended by the CMS C&A Evaluator in the ST&E Report, milestones and projected timeframes for completion of corrective actions, and projected costs associated with completion of corrective actions. ♦ Updates the SSP and attachments to reflect the actual state of the security controls after the security evaluation and completion of any corrective actions. ♦ Verifies the SSP and attachments contain an accurate list and description of the internal security controls and a description of the actual vulnerabilities in the system resulting from the ineffectiveness or absence of security controls and modifies the SSP and RA's to reflect the vulnerabilities and risk.	<u>Product</u>: • System CAP • Updated SSP Reference: • Final ST&E Report. • *CMS Reporting Standard for Security Testing*
9.	System Maintainer / Developer System Owner	Assemble and deliver the Security Certification Package. ➢ System Maintainer / Developer: ♦ Transmits the SSP and CAP(s) to System Owner using a delivery method appropriate under the circumstances. • Due to the sensitive nature of the SSP and CAP(s), will protect it in both electronic and hard copy format in accordance with CMS policy. ➢ System Owner: ♦ Assemble the Security Certification Package. ♦ Transmits the Security Certification Package to the Authorizing Official using a delivery method appropriate under the circumstances. • Due to the sensitive nature of the Security Certification	<u>Product</u>: • Security Certification Package. Reference: • *CMS Certification and Accreditation Methodology* • *CMS Systems Security Policy, Standards and Guidelines Handbook*

		Package, shall protect it in both electronic and hard copy format in accordance with CMS policy.	
10.	CMS C&A Evaluator	➢ CMS C&A Evaluator: ♦ Develops an accreditation recommendation for the system. ♦ Delivers the recommendation to SSG.	

2.4 Security Accreditation Phase

The Security Accreditation Phase comprises two tasks. These tasks determine if the actual residual risk to CMS operations or assets is acceptable based on the sensitivity level. A recommendation to approve or deny accreditation is presented to the Designated Approving Authority.

TASK	ROLES	RESPONSIBILITIES	PRODUCT & REFERENCE
		SECURITY ACCREDITATION DECISION	
1.	SSG	Determine the actual residual risk to CMS operations and assets based upon the confirmed vulnerabilities in the system, and any planned or completed corrective actions to reduce or eliminate those vulnerabilities. ➢ SSG: ♦ Reviews the Security Certification Package, and assesses the actual vulnerabilities identified by the CMS C&A Evaluator to determine how those vulnerabilities translate into actual risk to CMS operations and assets. ♦ Determines which system vulnerabilities are of greatest concern to CMS and which are not acceptable under any circumstances. ♦ Determines which vulnerabilities can be tolerated without creating an undue risk to CMS operations and assets. ♦ Reviews the corrective actions planned to address each vulnerability. ♦ Reviews the timeframe for completing corrective actions, and the costs associated with completing corrective actions in determining the business risk of each vulnerability. Consults the System Owner or the Senior Agency Information Security Official, or for an objective assessment, the CMS C&A Evaluator to determine the expected effectiveness of each planned corrective action. ♦ Develops the Actual Residual Risk Statement based on the	Product: • Actual Residual Risk Statement. Reference: • ST&E Report • SSP • CMS RA Methodology • CMS IS RAM • ARS

TASK	ROLES	RESPONSIBILITIES	PRODUCT & REFERENCE
		operation of the system in the proposed environment. The actual residual risk will form the basis for the security accreditation decision. ♦ Deliver the Actual Residual Risk Statement to the CIO.	
2.	CIO System Maintainer / Developer	Determine if the actual residual risk to CMS operations and assets is acceptable. ➢ CIO: ♦ Balances CMS business mission and operation requirements with the security considerations documented within the Security Certification Package. ♦ Reviews all information contained in the Security Certification Package, and, where appropriate, consults with key CMS officials, prior to rendering an accreditation decision. ♦ Authorizes, interim approval or refutes accreditation. • Issues a full authorization to operate the system in the proposed environment if the actual residual risk to CMS operations and assets are deemed acceptable. • Issues an interim approval to operate if the actual residual risk to CMS operations and assets are not deemed fully acceptable, but there is a strong CMS mission-related interest to place the system into operation. ▪ The interim approval shall be a limited authorization to operate under specific terms and conditions. ▪ The system is not accredited during the period of limited authorization to operate. ▪ Task the System Maintainer / Developer to complete certain corrective actions within a stated period of time.	

TASK	ROLES	RESPONSIBILITIES	PRODUCT & REFERENCE
		• Refuses accreditation if the actual residual risk to CMS operations and assets are deemed unacceptable, and the system shall not be authorized for operation. ➢ System Maintainer / Developer: ♦ Submits for approval a detailed plan of action and milestones to the CIO prior to the interim approval taking effect.	
		SECURITY ACCREDITATION DOCUMENTATION	
3.	SSG CIO	Prepares the final Security Accreditation Package, and transmits copies of the final Security Accreditation Package to the System Maintainer / Developer, System Owner and any other CMS officials having an interest in the security or operation of the system. ➢ SSG: ♦ Prepares the Accreditation Letter and Form. ♦ Delivers the letter and form with the Residual Risk Statement to the CIO. ➢ CIO: ♦ Reviews the Residual Risk Statement for the purpose of reviewing the letter and form for approval. ♦ Signs the Security Accreditation Decision Letter and Security Accreditation Form within the Security Accreditation Package. • The decision letter must include the accreditation decision, and identify any further actions the System Maintainer / Developer must take. • The Accreditation Form shall contain the terms and conditions for system operation, including required corrective actions, and any attachment the CIO wishes to provide to the System Maintainer / Developer. ➢ SSG: ♦ Assembles the Security Accreditation Package.	<u>Product</u>: • Residual Risk Statement • Security Accreditation Package Reference: • *CMS Certification and Accreditation Methodology* • Security Certification Package

TASK	ROLES	RESPONSIBILITIES	PRODUCT & REFERENCE
		♦ Transmits the Security Accreditation Package to the System Maintainer / Developer, System Owner and any other CMS official with an interest in the security or operation of the system using a delivery method appropriate under the circumstances. ♦ Retains one copy each of the Security Certification Package and Security Accreditation Package for the CIO. ♦ Retains one copy each of the Security Certification Package and Security Accreditation Package for storage in a secure, yet easily accessible location. • Due to the sensitive nature of the Security Certification Package, it shall be protected in both electronic and hard copy format in accordance with CMS policy.	
4.	System Maintainer / Developer Component ISSO	Update the SSP and CAP, if necessary, based upon the final determination of actual residual risk to CMS operations and assets. ➢ System Maintainer / Developer and Component ISSO: ♦ Updates the SSP and attachments to reflect any changes made to the system as a result of the Security Accreditation Phase. ♦ Notes in the SSP and attachments, any conditions set forth in the accreditation decision. • There should be minimal revisions to the SSP at this time.	<u>Product:</u> • Updated SSP • Updated CAP Reference: • Accreditation Package • Actual Residual Risk Statement.

2.5 Continuous Monitoring Phase

The Continuous Monitoring Phase provides DAA with regular updates on the status of the systems within the Authorizing Officials scope of authority. This phase enables the DAA to monitor effectively the viability and relevance of a system's existing accreditation.

The Continuous Monitoring Phase comprises three tasks. The change and configuration monitoring allows timely identification of major changes to the software of the system. The on-going testing of controls provides the data for the regular review of the internal controls of the system.

TASK	ROLES	RESPONSIBILITIES	PRODUCT & REFERENCE
		CONFIGURATION MANAGEMENT AND CHANGE CONTROL	
1.	System Maintainer / Developer	Use CMS configuration management and change control policies and procedures to document proposed or actual changes to the system. ➢ System Maintainer / Developer: ♦ Documents any relevant information about proposed or actual changes to the system hardware, firmware, or software. • Includes, at a minimum, software version or release numbers, descriptions of new or modified system features or capabilities, and information security implementation guidance. ♦ Documents any changes to the operating environment, including modifications to the physical environment.	Product: • Configuration Change document. Reference: • *CMS Software Quality Assurance Policy* ♦ *CMS Investment Management Policy*

TASK	ROLES	RESPONSIBILITIES	PRODUCT & REFERENCE
2.	System Maintainer / Developer Component ISSO SSG	Analyze the proposed or actual changes to the system to determine the security impact of such changes. ➢ System Maintainer / Developer: ♦ Assesses the potential security and functional impact of changes to the system. • Prior to performing this security impact assessment, do not make significant changes to the system. ➢ System Maintainer / Developer and Component ISSO: ♦ Develops a CAP to include all corrective actions necessary to reduce or eliminate (to an acceptable level) the resulting impacts from the changes if the Security Impact Assessment reveals that the changes to the system will affect the security of the system. • The CAP shall include descriptions of each planned corrective action, an assignment of responsibility for completing corrective actions, anticipated costs, and project milestones. ➢ SSG: ♦ Reviews the security impact assessment and the CAP to determine if the changes increase the system risk to an unacceptable level. • If the system risk level remains acceptable, the changes may proceed. • If the system risk level would become unacceptable, the Authorizing Official may revoke the system accreditation entirely or revoke the full accreditation and grant an interim approval.	<u>Product:</u> • Security Impact Assessment • A new CAP Reference: • Configuration Change document • *CMS Reporting Standard for Security Testing*

		ON-GOING SECURITY CONTROL VALIDATION	
3.	System Maintainer / Developer Component ISSO System Owner Senior Agency Information Security Official	➢ System Maintainer / Developer and Component ISSO: ♦ Identify a set of security controls to be monitored regularly reflecting CMS security priorities, and the importance of the system to CMS operations. ♦ Select those security controls whose compromise could result in the greatest harm to CMS operations and assets should be monitored. • For high-risk systems, a greater number and breadth of security controls shall be monitored on a regular basis. • A smaller number of security controls shall be monitored for low-risk system. ➢ System Owner and Senior Agency Information Security Official: ♦ Analyzes the Monitoring Process. ♦ Reviews, approves and / or modifies the selection of controls.	Reference: *CMS Information Security Levels*
4.	Component ISSO System Maintainer / Developer System Owner SSG	Evaluate the agreed-upon set of security controls in the system to determine the continued effectiveness of those controls in providing appropriate protection for the system. ➢ Component ISSO: ♦ Performs independent or internal security reviews, self-assessments, ST&E, penetration testing, or audits. ➢ System Maintainer / Developer: ♦ Employs standard evaluation procedures and techniques, similar to the certification ST&E procedures and techniques to determine the effectiveness of the security controls. • Employs more frequent and intensive techniques in security controls for high-risk systems. • Implements Security Controls to protect low-risk systems, which shall then be reviewed less often and in a less intensive manner.	<u>Product</u>: • Monitoring Process Report. • CAP (potential). Reference: • *CMS Reporting Standards for Security Tests* • NIST 800-53A. • ARS.

		♦ Documents the monitoring process for review by the System Owner. ➢ System Maintainer / Developer and Component ISSO: ♦ Develops a CAP and updates the SSP and attachments if the results of the evaluation reveal that certain controls are less effective than planned or expected, and affect the security of the system negatively. ♦ Delivers the CAP and updated SSP with attachments to the System Owner. ➢ System Owner: ♦ Deliver the CAP and updated SSP with attachments to the SSG. ➢ SSG: ♦ Review and approve on behalf of the CIO.	
STATUS REPORTING AND DOCUMENTATION			
5.	System Maintainer / Developer	Update the SSP based upon the documented changes to the system and the results of the on-going security control monitoring process. ➢ System Maintainer / Developer: ♦ Updates the SSP with the most current security-related information within five (5) business days after making a significant change to the system. ♦ Re-evaluates the system risk level designation during each update of the SSP.	<u>Product</u>: • Updated SSP Reference: • Monitoring Process Report • CAPs • *CMS Information Security Levels*
6.	System Maintainer / Developer System Owner	Report the security status of the system to the SSG. ➢ System Maintainer / Developer: ♦ Prepares and submits status reports to the System Owner, describing the continuous monitoring activities employed for the system and presenting a plan of action and milestones for reducing and eliminating any existing vulnerabilities within the system discovered during the security impact assessment or security evaluation. ♦ Bases the frequent status reports on the risk level of	<u>Product</u>: • Status Reports Reference: • Monitoring Process Reports • CAPs • ST&E Report • Accreditation Package

	SSG	system, as stated in the following: • High-risk systems' status reports are due every thirty (30) days. • Medium-risk systems' status reports must be submitted once every sixty (60) days. • Low- risk systems' status reports are submitted once every one hundred and eighty (180) days. ➢ System Owner: ♦ Provides SSG with status report summaries. ➢ SSG: ♦ Uses the status report summaries to monitor the security status of the system.	

2.6 Re-authorization Phase

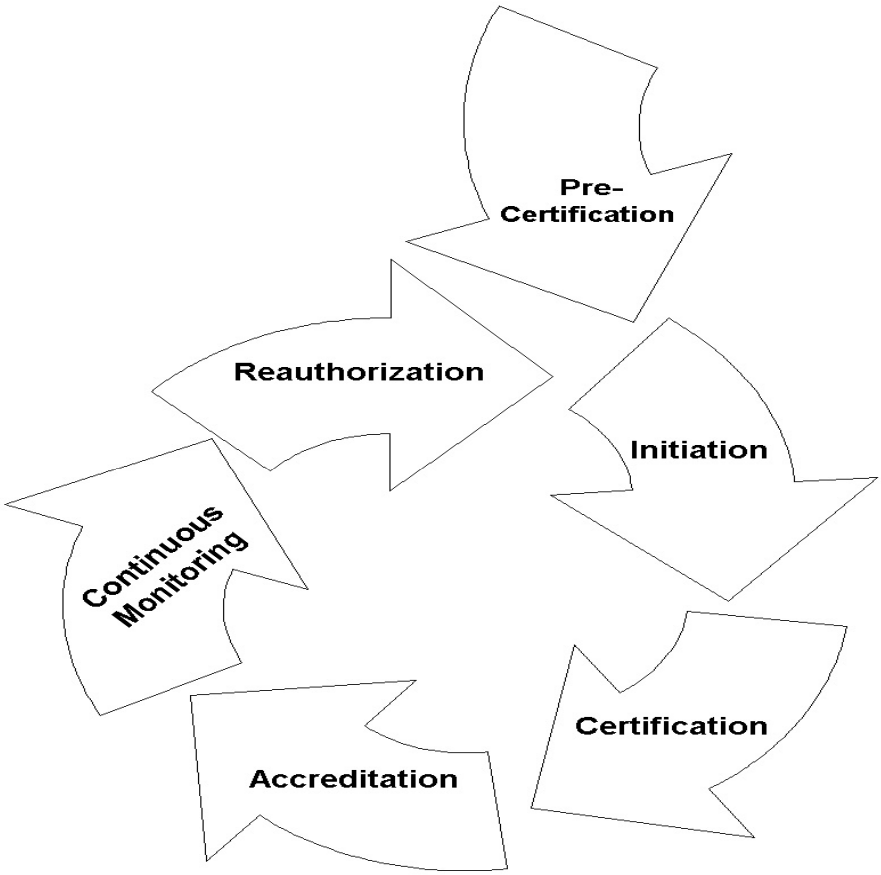
Re-authorization is necessary determine if CMS systems are continuing to operate at an acceptable risk level. Over the life of the system, many changes occur that may reduce the effectiveness of internal security controls. Security controls typically become outdated and less effective as threats and vulnerabilities evolve. The objective of the re-authorization tasks is to ensure that C&A is an on-going process, and that information security is managed throughout the life of a system.

TASK	ROLES	RESPONSIBILITIES	PRODUCT & REFERENCE
		RE-AUTHORIZATION DETERMINATION & NOTIFICATION	
1.	SSG	➢ SSG: ♦ Determines when re-authorization is necessary for a particular system. • This determination is based upon CMS requirements for regular re-authorization of systems, legislative and regulatory requirements for re-authorization of Federal systems, and whether significant changes have been made to an authorized system that may affect system security. ♦ Implements regular re-authorization of CMS systems in accordance with the *CMS Information Security Handbook.* • All medium- and high-risk systems shall be re-authorized at least once every five (5) years, or • When significant changes to the system adversely affect system security.	<u>Product</u>: • Re-certification Notification Reference: • *CMS Information Security Handbook* • Accreditation Package • Status Reports
		PERFORM SYSTEM RE-AUTHORIZATION	
2.	CIO	➢ CIO: ♦ Validates the current system accreditation for one-hundred eighty (180) days. ♦ Declares the operation of the system as unauthorized, if the system is not re-authorized at the expiration of one-hundred eighty (180) days.	<u>Product</u>: • Establish one-hundred eighty (180) day extension of current system accreditation; or • System is no longer authorized to operate.

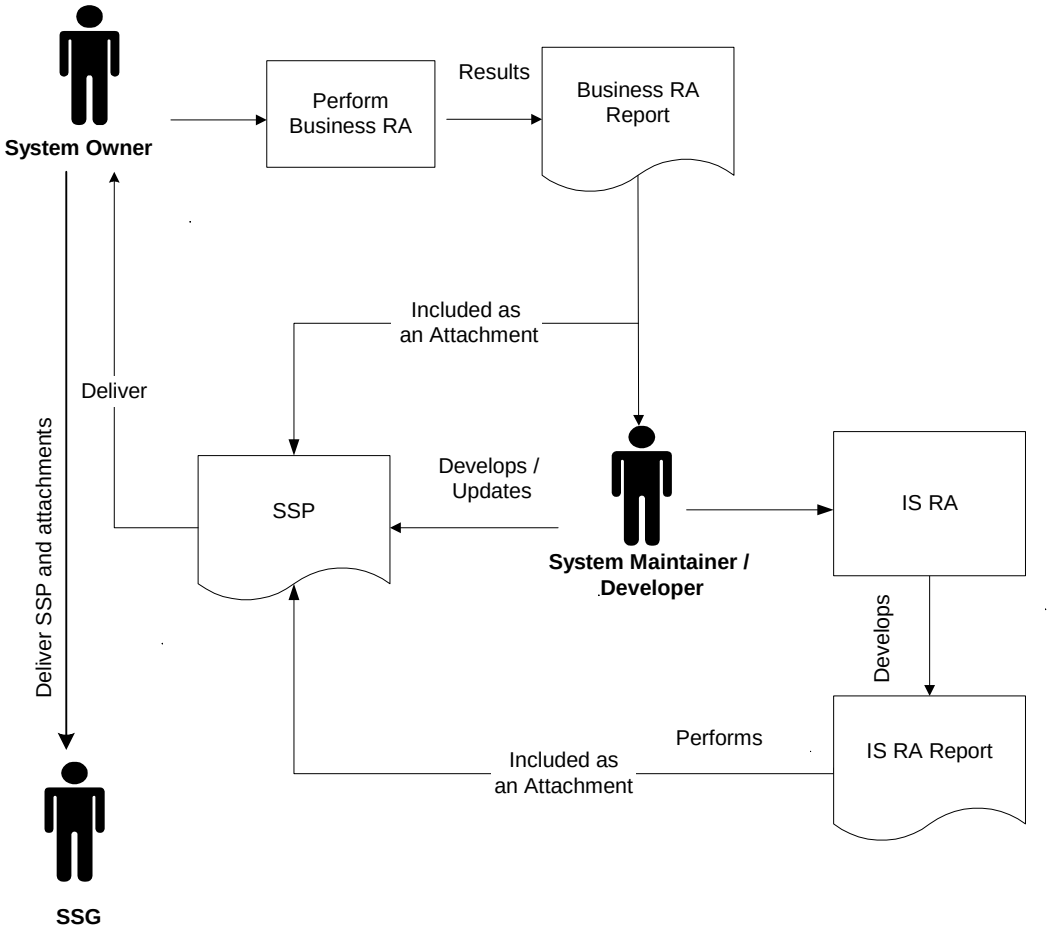
TASK	ROLES	RESPONSIBILITIES	PRODUCT & REFERENCE
3.	SSG	➢ SSG: ♦ Notifies the System Owner and System Maintainer / Developer, in writing, within five (5) business days. ♦ Begins the re-authorization process at the Initiation Phase of the CMS Certification and Accreditation Methodology.	

APPENDIX A –C&A FLOWCHARTS

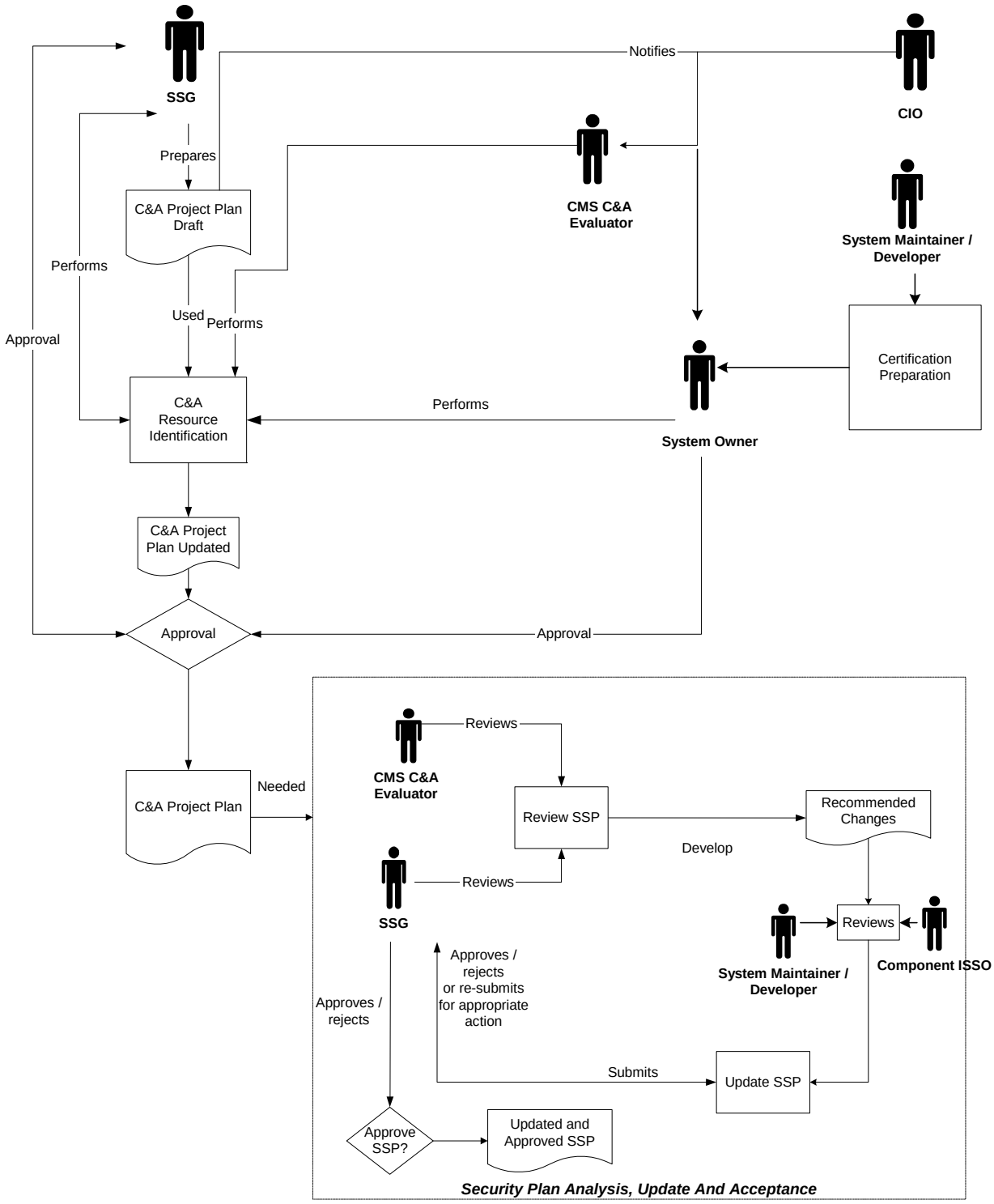
C&A PHASES



C&A PRE-CERTIFICATION PHASE

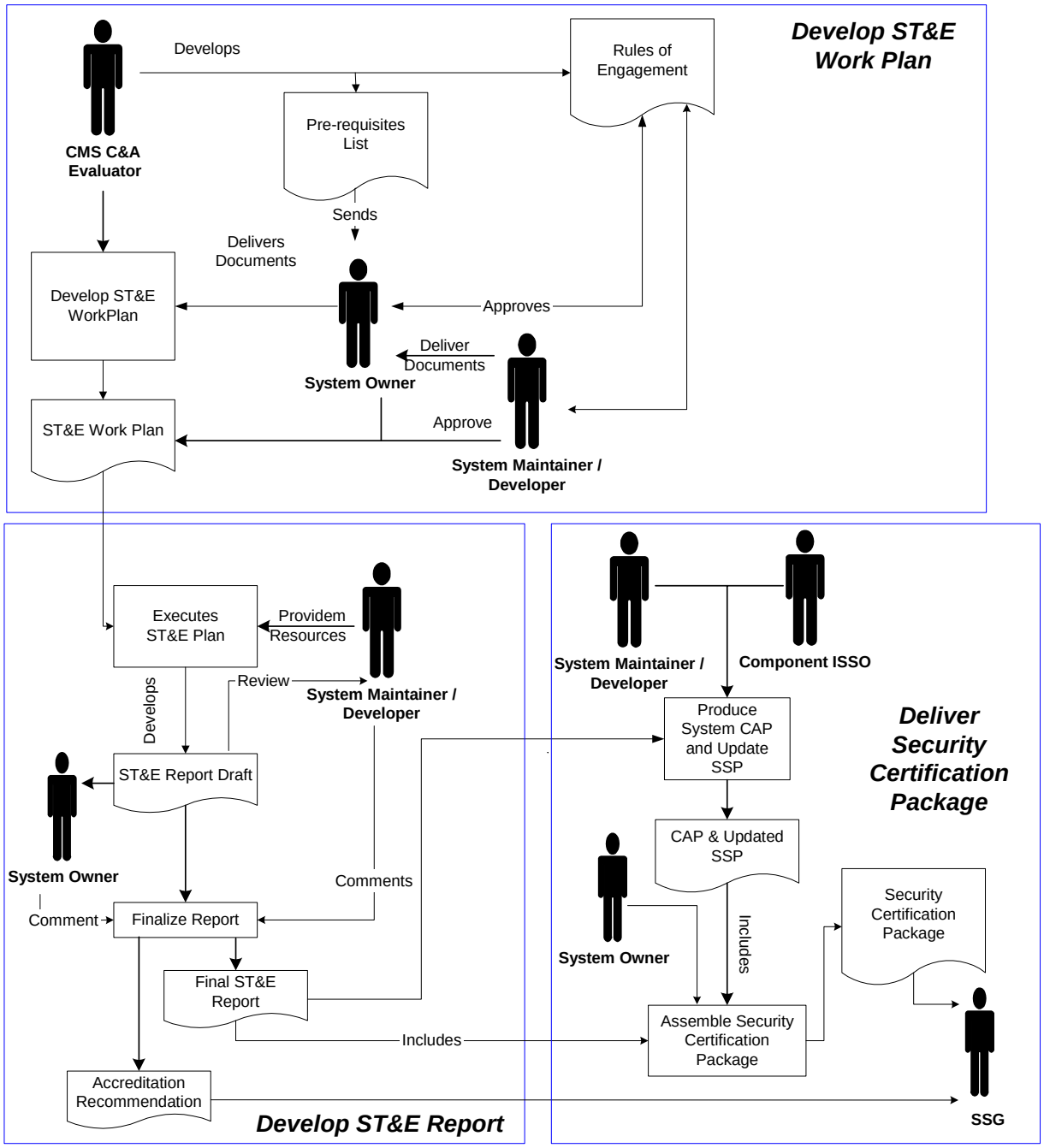


INITIATION PHASE[1]



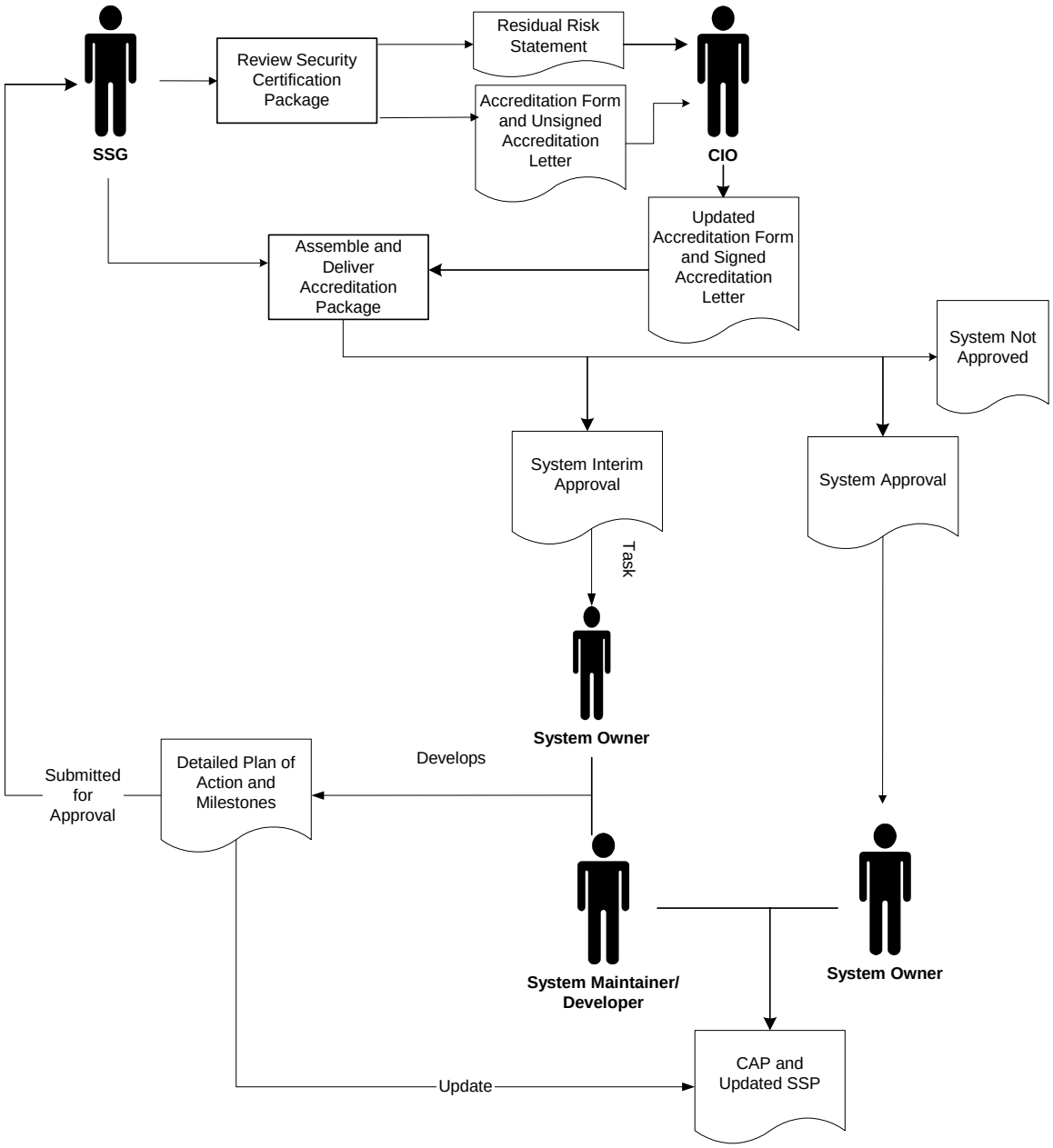
[1] In this figure, the viewer should regard updating the IS RA as an implicit activity associated with updating the SSP.

SECURITY CERTIFICATION PHASE[2]



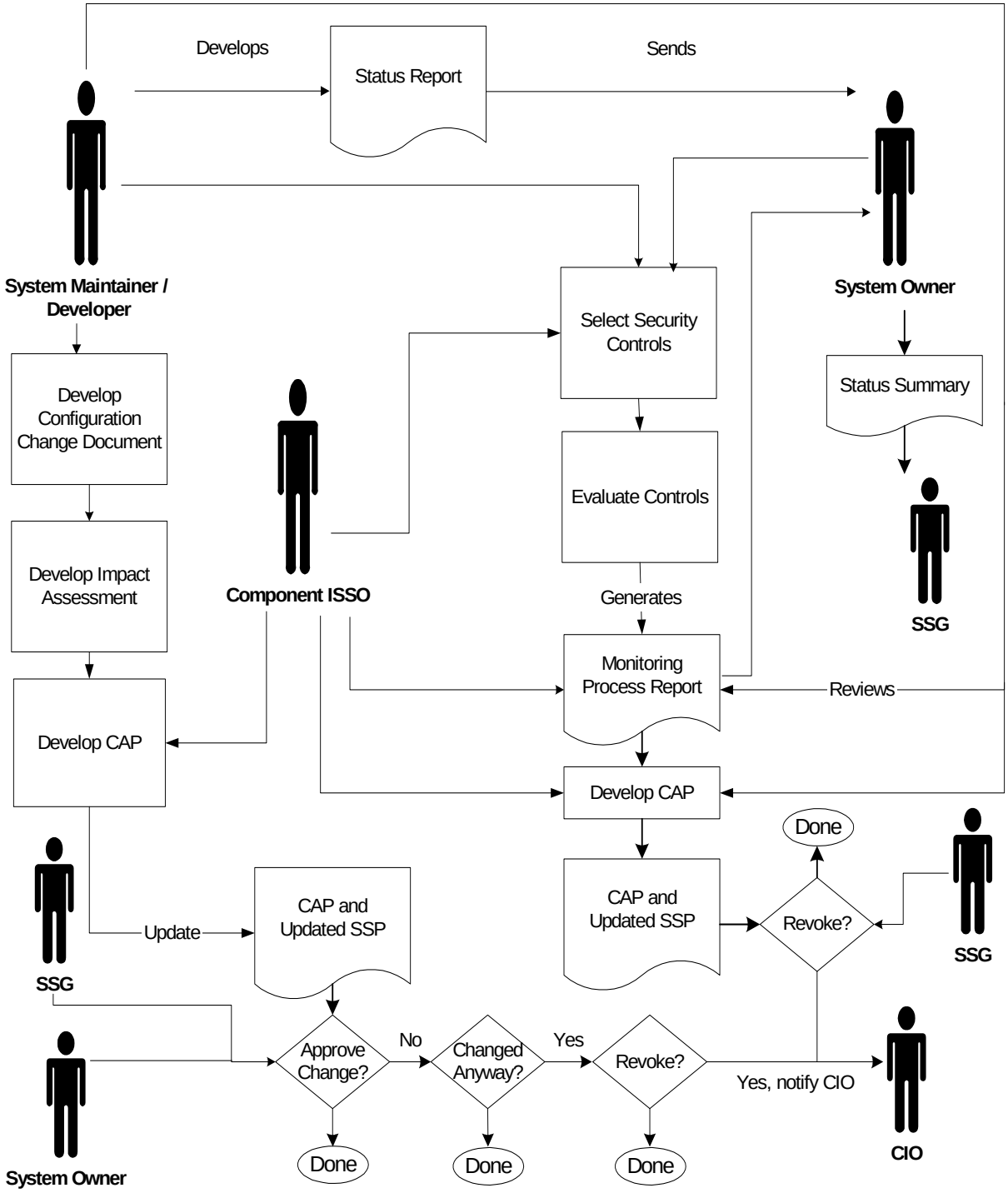
[2] In this figure, the viewer should regard updating the IS RA as an implicit activity associated with updating the SSP.

SECURITY ACCREDITATION PHASE[3]



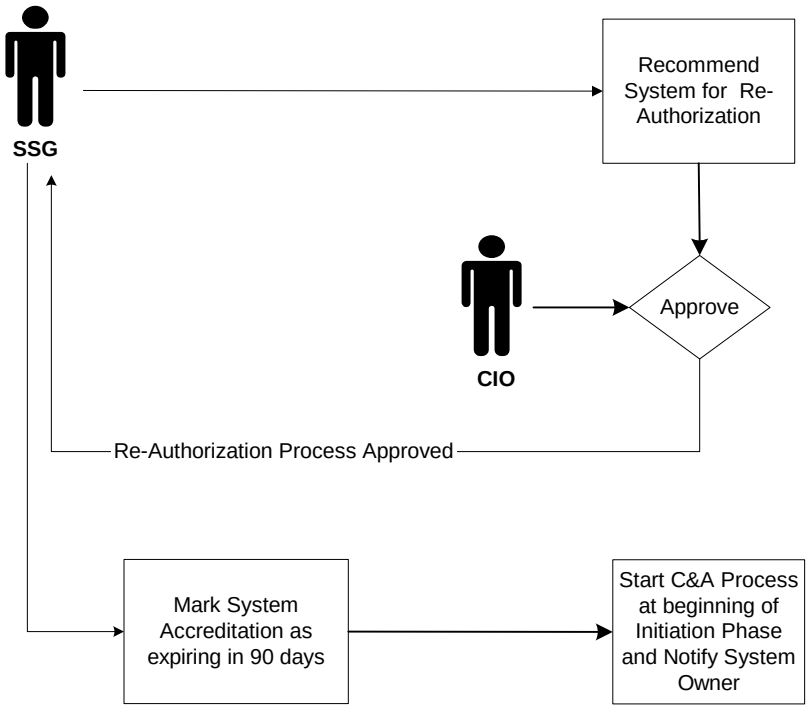
[3] In this figure, the viewer should regard updating the IS RA as an implicit activity associated with updating the SSP.

CONTINUOUS MONITORING PHASE[4]



[4] In this figure, the viewer should regard updating the IS RA as an implicit activity associated with updating the SSP.

RE-AUTHORIZATION PHASE



APPENDIX B – Certification Intensity Level

CMS must organize and utilize its security resources in an efficient and effective manner to maximize the benefit from limited resources. When working to reduce risk to the agency, CMS must utilize and expend resources in a fashion that is commensurate with the benefit the agency will derive from reducing that risk. Because the information security level of a system reflects the sensitivity level of that system, security certification activities must be commensurate with the information security level of the system and, thus, the risk to CMS assets, resources, and business processes. For C&A efforts, this means tailoring the scope of certification activities to the expected magnitude of harm that may result from compromise of the system.

In the CMS Information Security Level document, CMS defines three levels of system security: High, Moderate, and Low. For the C&A process, each of these security classification levels maps to a different certification intensity level (see table on next page). During the C&A Initiation Phase, the System Owner, System Maintainer / Developer and the CMS C&A Evaluator plan the scope of the certification process to tailor their certification activities to appropriate certification intensity level for the system.

Compromise of a high information security level system may impact significantly the ability of CMS to conduct mission critical agency business activities. An inability to conduct or complete a critical or mandatory business activity may have significant political and legal implications for CMS. Therefore, certifying a system that has a high information security level requires greater intensity of activity throughout the certification process. In high information security level systems CMS must perform certification activities at a high level of intensity (i.e., more intensive testing and evaluation), to verify that internal controls are effective in preventing unauthorized access or service disruption. Testing and evaluation for a system at this Certification Level requires a large resource commitment to ensure a thorough certification assessment. Conversely, a system with a low information security level carries an expectation of lower level of harm from compromise of the system. This lower level of risk allows the agency to perform the certification process at a lower level of intensity and less expenditure of resources. Likewise, certification intensity for a moderate level system would fall between the intensities necessary for high-level systems and low-level systems.

FISCAM Area/Topic	Low	Moderate (includes Low tests)	High (includes Low & Moderate tests)
Entity-wide Security Program Planning and Management (SP)			
SP-1 Periodically assess risks	• Verify that a Risk Assessment/Management Program is in place. • Verify that the program includes retention risks documentation	• Review Risk Assessment/Management policies. o Applies to all CMS related applications and systems o Includes regular revisits of RAs o Examine Roles and Responsibilities • Verify Risk Assessment/Management procedures exist.	• Review Risk Assessment/Management procedures. • Review random sample of RA documents for conformance to policy and procedure.
SP-2 Document an entity-wide security program plan	• Verify that security program is in place. • Verify security program plan indicates existence of relevant policies.	• Review security policies for to verify instantiation of appropriate controls: security awareness training, personnel controls, usage rules, etc. • Verify management approval of the program. • Verify process in place for review and revision of plan over time.	• Review security procedures. • Review process for maintenance of program plan. • Review most recent changes to plan.

FISCAM Area/Topic	Low	Moderate (includes Low tests)	High (includes Low & Moderate tests)
SP-3 Establish a security management structure and clearly assign responsibilities	• Verify that a security management structure is in place. • Verify that a security awareness program is in place. • Verify that incident response policy is in place.	• Review roles and responsibilities under the security management structure. • Security awareness program o Review program content. o Verify training record retention. • Incident response o Review policy for sufficiency. o Verify procedures are in place. o Verify retention of records.	• Review security awareness training records. • Verify users and owners are aware of and understand their responsibilities. • Review incident response procedures. • Review incident records for conformance to policy and procedure.
SP-4 Implement effective security related personnel policies	• Verify that HR policies include attention to security.	• Review HR policies to ensure inclusion of background checks, security in performance appraisals, etc. • Verify that HR procedures address security. • Verify retention of relevant security information (e.g., background checks).	• Review HR procedures to ensure inclusion of property return, notification to security, exit interviews, etc. • Verify background checks in place for all permanent personnel and contract personnel.
SP-5 Monitor the security program's effectiveness	• Verify that security program includes regular reassessment of program efficacy and	• Review security program policy and controls for revision of the security program.	• Review monitoring procedures. • Review most recent program

FISCAM Area/Topic	Low	Moderate (includes Low tests)	High (includes Low & Moderate tests)
and make changes as necessary	relevance. • Verify that security program assigns responsibility for update of program.	• Verify retention of program efficacy monitoring results.	changes.
Access Control (AC)			
AC-1 Classify information resources according to their criticality and sensitivity.	• Confirm policies and procedures exist for resource classification and related criteria that are based on: o Sensitivity o Confidentiality o Integrity o Availability • Verify that resource classifications are reviewed and approved by an appropriate senior official and have been recorded.	• Interview resource owners to verify their resource classifications are resultant of risk assessments. • Review resource documentation and compare to risk assessments to ensure the resource classifications reflect current conditions.	• Verify random selections of resources are classified to reflect risk assessment results and current conditions.
AC-2 Maintain a current list of authorized users and their access authorized.	• Verify access authorizations are: o Documented on standard forms and maintained on file; and o Approved by senior	• Verify access authorizations are securely transferred to security managers. • Review access authorization documentation for a selection of users with varying levels of access.	• Verify access authorization procedures for a random selection of users with varying levels and types (LAN, VPN, dial-up and otherwise) of access. • Verify, through testing, that

FISCAM Area/Topic	Low	Moderate (includes Low tests)	High (includes Low & Moderate tests)
	managers. • Verify policies and procedures are documented for varying types of access (LAN, VPN, dial-up and otherwise). • Verify procedures exist to document security profile changes. • Verify user termination and transfer policies and procedures exist. • Verify emergency and temporary access authorizations are: o Documented on standard forms and maintained on file; and o Securely communicated to the security function; and	• Review authorization and justification documentation for a selection of users with dial-up access. • Interview security managers and review documentation provided to them. • Review a selection of recent profile changes and activity logs. • Review user termination and transfer policies and procedures. • Verify emergency and temporaraty access authorizations are: o Securely communicated to the security function; and o Automatically terminated after a predetermined period.	unusual activity is investigated. • Verify that a random selection of terminated and / or transferred users were terminated or transferred promptly. • Test the access differences between the types of users: o Daily authorized users; o Temporary users; and o Emergency users.
AC-2 (Cont'd)	o Automatically terminated after a predetermined period. • Verify the use of standardized forms to document archiving,	• Compare the differences between authorized daily users and: o Emergency authorizations;	

FISCAM Area/Topic	Low	Moderate (includes Low tests)	High (includes Low & Moderate tests)
	deleting, or sharing of data files. • Review examples of documents or agreements regarding how data or programs are shared with other entities and how they are protected.	and o Temporary authorizations. • Interview data owners regarding their experiences with past and present procedures for file sharing and file sharing agreements.	
AC-3 Establish physical and logical controls to prevent or detect unauthorized access. (*These audit procedures should be coordinated with section SC-2 since many of the control objectives and techniques are the same.*)	• Verify facilities housing sensitive and critical resources have been identified. • Review diagrams of the physical layout of the following facilities: o Computer; o Telecommunications; and o Heating and cooling system. • Review risk analysis. • Review lists of individuals authorized access to sensitive areas and determine the appropriateness for access according to their level of responsibility. • Observe entries and exits from facilities during and after	• Walk through the facilities for review, comparison to documentation and preliminary testing of controls in place. • Observe utilities' access paths. • Interview management in regards to facility security policies and procedures. • Observe entries and exits from sensitive areas during and after normal business hours and verify that keys, other devices or visible identification are required to enter the areas. • Select random entries within the log of withdrawals and returns, verify the existence of	• Test perimeter controls prior to identification as an auditor. • Interview random employees in regards to facility security policies and procedures and actual practices. • Physically test the procedures for media removal from storage or sensitive areas. • Observe a fire drill and the actual practices of the facility employees and security personnel. • Interview guards at facility entry. • Attempt to gain access to facilities as an unscheduled visit without justification for access to test perimeter

FISCAM Area/Topic	Low	Moderate (includes Low tests)	High (includes Low & Moderate tests)
	normal business hours and verify that keys, other devices or visible identification are required to enter facilities. • Review policies and procedures for the removal and return of storage media from and to the library.	the tape or other media, and determine whether proper authorization was obtained for the movement. • Observe practices for safeguarding keys and other devices. • Verify emergency exit and re-entry procedures exist to ensure only authorized personnel are allowed to reenter after fire drills, etc.	security procedures and actual practices. • Evaluate biometrics or other technically sophisticated techniques by obtaining the assistance of specialists.
AC-3 (Cont'd)	• Review written emergency procedures and examine documentation supporting prior fire drills. • Verify visitor entry logs exist, are mandatory and are routinely reviewed. • Review documentation on and logs of entry code changes. • Review the policies and procedures governing the authentication process for visitors, contractors and maintenance personnel. • Review password policies and	• Verify visitors to sensitive areas are formally signed in and escorted. • Review the visitor entry logs. • Verify entry codes are changed periodically. • Observe users keying in passwords and verify password procedures enforce the following: o Unique for specific individuals, not groups; o Controlled by the assigned user and not subject to disclosure; and	• Interview users in regards to passwords, tokens or other devices to identify and authenticate. • Attempt to log on without a valid password; make repeated attempts to guess passwords to verify controls.

FISCAM Area/Topic	Low	Moderate (includes Low tests)	High (includes Low & Moderate tests)
	verify that they are: o Unique for specific individuals, not groups; o Controlled by the assigned user and not subject to disclosure; and o Changed periodically; and o Not displayed when entered; and o At least 6 alphanumeric characters in length; and o Prohibit from reuse at least 6 generations.	o Changed periodically; and o Not displayed when entered; and o At least 6 alphanumeric characters in length; and o Prohibit from reuse at least 6 generations. • Verify the use of names or words in passwords is prohibited and vendor-supplied passwords are replaced through the use of password audit software.	
AC-3 (Cont'd)	• Review access path diagrams. • Review security software parameters. • Verify naming conventions are used for resources.	• Verify the use of a generic User ID is prohibited. • Verify attempts to log on with invalid passwords are limited to 3-4 attempts. • Review security logs after numerous attempts to log on with invalid an invalid user ID and password. • View dump of password files (e.g., hexadecimal printout). • Interview security administrators and system	• Using ethical hacking methods during external penetration tests, attempt to utilize exploits to verify controls are in place to prevent the compromise of the confidentiality, integrity and availability of data and / or resources.

FISCAM Area/Topic	Low	Moderate (includes Low tests)	High (includes Low & Moderate tests)
		users in regards to logical controls over data files and software programs. • Verify security software is used to restrict access. • Verify terminals and personal computers automatically log off after a period of inactivity. • Verify inactive user accounts are monitored and removed when not needed. • Conduct penetration tests that expose vulnerabilities to key resources and critical data.	
AC-3 (Cont'd)	• Determine library names for sensitive or critical files and libraries and obtain security reports of related access rules. • Using access rules reports, determine who has access to critical files and libraries and whether the access matches the level and type of access authorized. • Review policies and procedures for logical controls over databases.	• Conduct penetration tests in the following roles: o As an "outsider" with no information about the entity's computer system; and o As an "outsider" with prior knowledge about the systems – e.g., an ex-insider; and o As an "insider" with and without specific information about the	

FISCAM Area/Topic	Low	Moderate (includes Low tests)	High (includes Low & Moderate tests)
	• Review policies and procedures for telecommunications access.	entity's computer systems and with access to the entity's facilities. • When conducting external penetration tests as an "outsider" or an "insider", test the controls over access to computer resources, including networks, dial-up, LAN, WAN, RJE, and the Internet. • Using ethical hacking methods during internal penetration tests, attempt to us an ID with no special privileges to attempt to gain access to computer resources beyond those available to the account.	
AC-4 Monitor access, investigate apparent security violations, and take appropriate remedial action.	• Verify logs of activity involving access to and modifications of sensitive or critical files exist. • Review the policies and process of management notification of actual security violations and activities, including: o Failed access attempts;	• Interview personnel responsible for clearing equipment and media for reuse • Review security software settings to identify types of activity logged. • Test a selection of security violations to verify that follow-up investigations	• Test the security software's ability to identify types of activity by utilizing an assigned user account.

FISCAM Area/Topic	Low	Moderate (includes Low tests)	High (includes Low & Moderate tests)
	o Sensitive activity; and o Detected unauthorized access. • Review security violation reports. • Review documentation showing reviews of questionable activities. • Interview senior management and personnel responsible for summarizing violations and review any supporting documentation. • Examine policies and procedures regarding suspicious activity investigation and remedial action policy change and review.	were performed and to determine what actions were taken against the perpetrator.	
Application Software Development and Change Control (CC)			
CC-1 Processing features and program modification	• Verify the software development policies are in place; e.g., SDLC and	• Review software development policies. • Verify software development	• Review software development procedures. • Review random sample of

FISCAM Area/Topic	Low	Moderate (includes Low tests)	High (includes Low & Moderate tests)
s are properly authorized.	management authorization for changes. • Verify policy in place on use of public domain and personal software. • Verify retention of relevant documents and approvals.	procedures are in place. • Review policy on public domain and personal software. • Verify procedures on public domain and personal software in place.	software development documents and approvals for conformance to policy and procedure. • Review procedures on public domain and personal software in place.
CC-2 Test and approve all new and revised software.	• Verify policies in place on software testing. o Standard changes. o Emergency changes. • Verify retention of testing results documentation.	• Review policies on software testing. o Standard changes. o Emergency changes. • Verify procedures on software testing and change management. o Standard changes. o Emergency changes. • Verify policy in place on software change migration. • Verify retention of software change migration documentation and approvals.	• Review procedures on software testing. o Standard changes. o Emergency changes. • Review random sample of testing results documentation for conformance to policy and procedure. • Review random sample of software migration documentation and approvals for conformance to policy and procedure.
CC-3 Control software libraries.	• Verify policy in place for maintenance of software inventory. • Verify software change	• Review software inventory policy. • Verify software inventory procedures are in place.	• Review software inventory procedures. • Examine a random sample of entries from the inventory for

FISCAM Area/Topic	Low	Moderate (includes Low tests)	High (includes Low & Moderate tests)
	management policy is in place. • Verify access controls in place for production application software libraries.	• Review software change management policy. • Verify software change management procedures are in place.	accuracy. • Review change management procedures. • Verify software change management function is independent of software development functions.
System Software (SS)			
SS-1 Limit access to system software.	• Review site's policies relevant to the ARS and FISMA control requirements. • Verify that site has Continuity and Contingency Plans (refer to NIST 800-34). • Review Risk Assessments, recent audits and test reports of the various systems, GSSs and MAs and verify the following controls and / or procedures are in place: o An SSP for each system exists; and o Corrective Action Plans for each vulnerability exists; and o Vulnerability tracking	• Verify the presence of standard network safeguards such as: o DMZs; o Firewalls between Intra- and Extra-nets; o Firewalls between the Intranets and the Internet; and o Firewalls between production and non-production Intranets; and o Policies, rule sets and filter sets exist for firewalls, routers and switches and are adequate to prevent access of networks with differing	• Use social engineering techniques to attempt to gain access. • Perform network scanning that, at a minimum, is comparable to the ISS Internet Security Scanner policy levels L3 and L4. • For a representative sample of hosts and servers that support the system, using a site supplied low-level (i.e., limited authority) User ID: o Attempt to manipulate the host / server's security system ▪ Attempt to invoke security system

FISCAM Area/Topic	Low	Moderate (includes Low tests)	High (includes Low & Moderate tests)
	policy and procedure is in place and utilized; and o Audit trails include user rights and privileges and access records; and o User ID rights and privileges are assigned according to sensitivity and security levels; and	sensitivity levels. • Engage in "dumpster diving" to locate sensitive data, User IDs, or passwords. • Attempt to use common, standard, or default User IDs to access representative sample of: o Hosts and servers that support the system; and	administration tools, ▪ Attempt to create a new power-, super-, root-, or administrative user, and ▪ Attempt to alter security system parameters; o Attempt to view sensitive or confidential material on the host / server's output queues; and
SS-1 (Cont'd)	o Each system, GSS and MA operate as intended, safely and securely; and o Backup procedures ensure the confidentiality, integrity and accessibility of critical data. • Analyze the site's Internet footprint (using ARI or other public domain databases).	o Hosts and servers with network (both direct and indirect) connections to the hosts and servers that directly support the system. • For a representative sample of hosts and servers that support the system, using a site supplied low-level (i.e., limited authority) User ID: o Check service log-ons, such as telnetting to the default gateway, FTP on servers, and zone transfers.	o Attempt to access sensitive Medicare files. • Attempt to steal or crack passwords using sniffers and password crackers. • Attempt to create false trust relationships and access sensitive network user lists.

FISCAM Area/Topic	Low	Moderate (includes Low tests)	High (includes Low & Moderate tests)
		• Review User ID's actual access to the system's data files, software libraries, and directories. • Attempt to use common, standard, or default User IDs to access a sampling of end-user or desktop systems.	
SS-1 (Cont'd)		• For a representative sample of hosts and servers that support the system: o Review host / server's system software configuration settings; o Review a site supplied low-level (i.e., limited authority) User ID's actual access to the system software data files, libraries, and directories; and o Test a site supplied low-level (i.e., limited authority) User ID's ability to issue system operation commands. • For a representative sample of	

FISCAM Area/Topic	Low	Moderate (includes Low tests)	High (includes Low & Moderate tests)
		hosts and servers with network (both direct and indirect) connections to the hosts and servers that directly support the system review the host / server's system software configuration settings. • Tests to determine intrusion detection capability of site.	
SS-1 (Cont'd)		• For a representative sample of routers, proxy servers, firewalls, etcetera that support the system, review the devices' configuration settings. • War-dial site's network. o Identify presence of modem tones. o Attempt to gain access through common, standard, or default User IDs (if successful, document and cease activity). • For all routers, proxy servers, firewalls, etcetera that support the system, review the devices' configuration settings.	

FISCAM Area/Topic	Low	Moderate (includes Low tests)	High (includes Low & Moderate tests)
		• For a representative sample of routers, proxy servers, firewalls, etcetera that connect to the network devices that support the system, review the devices' configuration settings. • Use brute force attacks to log-in to network servers. • Internal network testing (both manual and automated) on Medicare specific systems and network. infrastructure.	
SS-1 (Cont'd)		• Security penetration test of any processing platforms supporting Medicare specific data. • Perform automated scanning of site's Internet points of presence and other external network connections. Perform this activity at a level comparable to ISS Internet Scanner levels L1-L2. • Security penetration testing controls over LAN/WAN/Internet connections of relevant servers.	

FISCAM Area/Topic	Low	Moderate (includes Low tests)	High (includes Low & Moderate tests)
		• For all of hosts and servers that support the system: o Review host / server's system software configuration settings; o Review a site supplied low-level (i.e., limited authority) User ID's actual access to the system software data files, libraries, and directories; and o Test a site supplied low-level (i.e., limited authority) User ID's ability to issue operation commands.	
SS-2 Monitor access to and use of system software.	• Verify policy in place on use and monitoring of sensitive system functions and utilities. o Authorization of usage. o Monitoring of usage. o Investigation of incidents.	• Review policy on use and monitoring of sensitive system functions and utilities. o Authorization of usage. o Monitoring of usage. o Investigation of incidents. • Verify procedures are in place for monitoring use of sensitive system functions and utilities.	• Review procedures are in place for monitoring use of sensitive system functions and utilities. • Review a random sample of documentation, monitoring, and investigation results for sensitive system functions and utilities for conformance to policy and procedure.

FISCAM Area/Topic	Low	Moderate (includes Low tests)	High (includes Low & Moderate tests)
		o Authorization of usage. o Monitoring of usage. o Investigation of incidents. • Verify retention of documentation, monitoring, and investigation results for sensitive system functions and utilities.	
SS-3 Control system software changes.	• Verify policies in place on system software testing. o Standard changes. o Emergency changes. • Verify retention of testing results documentation. • Verify retention of relevant documents and approvals.	• Review policies on system software testing. o Standard changes. o Emergency changes. • Verify procedures on system software testing and change management. o Standard changes. o Emergency changes. • Verify policy in place on system software change migration. • Verify retention of system software change migration documentation and approvals.	• Review procedures on system software testing and change management. o Standard changes. o Emergency changes. • Review random sample of system software testing results documentation for conformance to policy and procedure. • Review random sample of system software migration documentation and approvals for conformance to policy and procedure.
Segregation of Duties (SD)			

FISCAM Area/Topic	Low	Moderate (includes Low tests)	High (includes Low & Moderate tests)
SD-1 Segregate incompatible duties and establish related policies.	• Verify policies and procedures for segregating duties exist and: o Are up-to-date; o Offer adequate compensating controls when resources are limited; o Ensure data processing personnel are not users of information systems; and o Ensure data processing personnel and security managers do not initiate, input or correct transactions; o Adequately document day-to-day operating procedures for the data center; o Identify prohibited actions; and o Document job descriptions and define requirements to fill positions. • Review agency organizational charts showing IS functions and assigned personnel. • Review relevant alternate or	• Interview management and IS personnel regarding segregation of duties. • Verify that organizational charts are correct by determining whether different individuals staff each function. • Observe activities of personnel to determine the nature and extent of the compliance with the intended segregation of duties. • Interview management and observe activities to verify compensating controls if resources are limited which prevent complete segregation of duties. • Interview personnel to verify their understanding of their duties and responsibilities and whether additional duties are undertaken that are not listed in their job descriptions. • Verify controls are in place to restrict access by job position in key operating and programming activities.	• Test transactions to verify controls are in place to ensure duties are segregated while not impeding function. •

FISCAM Area/Topic	Low	Moderate (includes Low tests)	High (includes Low & Moderate tests)
	backup assignments and determine whether the proper segregation of duties is maintained.		
SD-2 Establish access controls to enforce segregation of duties.	(*Note: Audit steps in this section are to be conducted in conjunction with Access Control (AC) audit steps.*) • Select documents or actions requiring supervisory review and approval for evidence of such performance. • Verify reviews are conducted and review the documentation to assess the adequacy of duty segregation.	• Interview management and subordinate personnel to verify physical and logical access controls help to restrict employees to authorized actions based upon job responsibilities.	• (*Examination of personnel review documentation is to be conducted in conjunction with Entitywide Security Program Planning and Management (SP) audits.*)
SD-3 Control personnel activities through formal operating procedures and supervision and review.	• Verify the following documents exist: o Written instructions for performance of work; o Operator instruction manuals for system operation; and o Application-run manuals on operating specific applications. • Review history log reports for	• Interview supervisors and personnel to determine the adequacy of the instruction manuals. • Observe processing activity to verify compliance with manual instructions and accuracy / applicability of instructions. • Determine what steps are followed to monitor console activity during processes.	• Test to verify operators are prevented from overriding file label or equipment error messages. • Test to determine if it is possible and / or whether operators override the IPL parameters.

FISCAM Area/Topic	Low	Moderate (includes Low tests)	High (includes Low & Moderate tests)
	signatures indication supervisory review. • Determine who is authorized to perform the initial program load for the system and verify that it is consistent with policy.		
Service Continuity (SC)			
SC-1 Assess the criticality and sensitivity of computerized operations and identify supporting resources.	• Review policies and procedures. • Verify lists of critical operations and data exist and document that: o Prioritizes data and operations; o Is approved by senior program managers; o Reflects current conditions; and o Identify supporting resources. • Review emergency processing priorities documentation. • Verify documentation has been reviewed and approved by appropriate program and data	• Interview program, data processing, and security administration officials to determine their input and their assessment of the reasonableness of priorities established.	

FISCAM Area/Topic	Low	Moderate (includes Low tests)	High (includes Low & Moderate tests)
	processing managers.		
SC-2 Take steps to prevent and minimize potential damage and interruption.	• Review written policies and procedures for backing up files. • Verify up-to-date system and application documentation are maintained at the off-site storage location. • Verify the backup storage site is: o Geographically removed from the primary site(s); and o Protected by environmental controls and physical access controls. • Examine the entity's facilities to verify implementation of environmental controls. • Determine whether heat and smoke detectors will notify the fire department. • Verify that environmental controls are periodically tested and review testing documentation.	• Compare inventory records with the files maintained off-site and determine the age of these files. • Locate and examine the backup files to verify that they can be used to recreate current reports. • Verify steps in the policies and procedures are followed. • Observe that operations staff are aware of the locations of devices and / or controls they may be expected • Observe whether water damage is possible and detectors are in place. • Verify that all data center employees have received training and understand their emergency roles and responsibilities.	• (*Environmental controls audits should be performed in conjunction with Access Control (AC) audits, regarding physical access controls.*)

FISCAM Area/Topic	Low	Moderate (includes Low tests)	High (includes Low & Moderate tests)
	• Verify policies and procedures exist for eating, drinking and other behavior that may damage computer equipment.		
SC-2 (Cont'd)	• Review policies and procedures for emergency response and contingency processes. • Review policies and procedures regarding hardware maintenance, problem management and change management. • Verify records / logs for the following exist: o Regular and unscheduled maintenance performed; o Actual performance in meeting service schedules; and o Problems and delays encountered, the reason, and elapsed time for resolution.	• Interview data processing, user and senior management to confirm: o Effective hardware maintenance, problem management, and change management help prevent unexpected interruptions; o Senior management takes measures to periodically to ensure user departments' needs are being met; and o Advance notification on hardware changes is given to users so that service is not unexpectedly interrupted.	
SC-3 Develop and document a comprehensive	• Verify a contingency plan has been documented that: o Reflects current conditions;	•	•

FISCAM Area/Topic	Low	Moderate (includes Low tests)	High (includes Low & Moderate tests)
contingency plan	o Has been approved by key affected groups; o Clearly assigns responsibilities for recovery; o Includes detailed instructions for restoring operations; o Identifies the alternate processing facility and the backup storage facility; o Includes procedures to follow when the data/service center is unable to receive or transmit data; o Identifies critical data files; o Is detailed enough to be understood by all agency managers; o Includes computer and telecommunications hardware compatible with the agencies needs; and o Provides for backup personnel so that it can be implemented independent		

FISCAM Area/Topic	Low	Moderate (includes Low tests)	High (includes Low & Moderate tests)
	of specific individuals. o Has been distributed to all appropriate personnel.		
SC-3 (Cont'd)	• Verify the contingency plan is periodically reassessed and, if appropriate, revised to reflect changes in hardware, software, and personnel. • Confirm several copies of the current contingency plan are securely stored off-site at different locations • Verify contracts and interagency agreements that establish a backup data center and other needed facilities: o Are in a state of readiness commensurate with the risks of interrupted operations; o Have sufficient processing capacity; and o Are likely to be available for use. • Review the contingency plan and compare its provisions with the most recent risk	• Interview senior management, data center management, and program managers to confirm actual provisions for each of the required items in the contingency plan exist. .	

FISCAM Area/Topic	Low	Moderate (includes Low tests)	High (includes Low & Moderate tests)
	assessment and with a current description of automated operations.		
SC-4 Periodically test the contingency plan and adjust it as appropriate.	• Review policies on testing. • Verify a "lessons learned" report exists from past testing experiences. • Review and documentation supporting contingency plan adjustments.	• Review documented test results.	• Observe a disaster recovery test.

APPENDIX C - ACRONYMS

ACRONYM	DEFINITION
ARS	Acceptable Risk Safeguards
C&A	Certification and Accreditation
CAP	Corrective Action Plan
CIO	Chief Information Officer
ISSO	Information System Security Officer
IS RA	Information Security Risk Assessment
IS RAM	Information Security Risk Assessment Methodology
ISS	Internet Security Systems
LAN	Local Area Network
NIST	National Institute of Standards and Technology
QA	Quality Assurance
RA	Risk Assessment
RAM	Risk Assessment Methodology
SDLC	System Development Life-Cycle
SSG	Security Services Group
SSP	System Security Plan
ST&E	System Test and Evaluation
VACAP	Vulnerability Assessment Corrective Action Process
WAN	Wide Area Network

APPENDIX D - C&A Methodology Groups and Procedural Roles

METHODOLOGY GROUP	PROCEDURAL ROLE	HIGH-LEVEL RESPONSIBILITY
Signatory Officials[5]	CIO	♦ Overall responsibility and authority for the C&A program. ♦ Authorizes system operation and signs Accreditation Package.
	DAA	♦ If assigned by the CIO, authorizes operation and signs the Accreditation Package by the authority of the CIO. ♦ "This authority has not yet been delegated." (March 10, 2004)
	System Owner	♦ Compiles and reviews the Certification Package and supporting documents. ♦ Certifies that the controls implemented for the system are adequate to meet agency policy and C&A requirements. ♦ Signs and approves the Certification Package
Senior Agency Information Security Officer	Director SSG (Senior Agency Information Security Official)	♦ Serves under the authority of the CIO in the C&A process. ♦ Performs the CIO's day-to-day C&A related tasks. ♦ Selects CMS C&A Evaluator and oversees Evaluators performance. ♦ Consults on authorizing decisions concerning CMS security policy and procedure. ♦ Reviews and facilitates the development of Information Security Certification Packages and Accreditation Packages. ♦ Collaborates with the System Owner to facilitate the approval of the Security Certification Package.
System Owners	System Owner	♦ Responsibility for the security of the system. ♦ Serves as liaison between Senior Agency Information Security Official and the

[5] Referred to as Authorizing Official in initial drafts of the C&A Methodology.

		System Maintainer / Developers and Component ISSO / SSO. ♦ Completes the Business RA. ♦ Responsible for the development of the SSP, Business RA and IS ♦ Correlates internal and external initiated audit information for the C&A process. ♦ Creates CAPs in collaboration with the Component ISSO and System Maintainer / Developer.
	System Maintainer / Developer	♦ Conducts the IS RA. ♦ Incorporates security controls in the system. ♦ Provides technical input for SSP, Risk Assessments and Corrective Action Plans (CAPs). ♦ Enhances security controls from the CAPs on the system.
ISSOs	Component ISSO / SSO	♦ Collaborates with the System Maintainer / Developer to ensure security controls conform to CMS policy and fulfill C&A requirements. ♦ Consults in creating CAPs. ♦ Periodically validates the security controls to ensure they are implemented in accordance with the system documentation.
CMS C&A Evaluators	CMS C&A Evaluator	♦ Conducts ST&E testing (develop test plan, execute test plan, and develop ST&E report in conjunction with updating the CMS Vulnerability Assessment Corrective Action Plan (VACAP) database). ♦ Develops system Certification recommendation based on the test results. ♦ Develops system Accreditation recommendation in collaboration with SSG from results of the testing.